Privacy Implications of Using AI Note-Takers at Work

Scott Foote

Last Updated: 8 December, 2025

Phenomenati Consulting
6 Liberty Square, #2736
Boston, MA 02109
(508) 709-7990 (office)
(617) 404-9419 (fax)

www.phenomenati.com

This page intentionally left blank.

Contents

1 Executive Summary

As the DPO, CISO, and/or CAIO for multiple organizations with staff across the US and Europe, the topic of **AI note-takers** and **Privacy** comes up literally every week.

Specifically, the question of the **legal** and **regulatory obligations**[1][2] for providing ***Notice***[3] and getting ***Consent***[4][5][6] prior to making a **recording** of either online or in-person meetings (e.g., **using an AI meeting notetaker** like Granola, Otter, Fireflies, MeetGeek, Krisp, Lindy, Read AI, or others). "*State laws on recording conversations – often addressed as* ***criminal*** ***eavesdropping*** *and* ***wiretapping*** *– vary significantly. Employers must understand this legal landscape when assessing a range of recoding issues.*"[7]

Full disclosure, this author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

But the short answer: if you have people in both the US and Europe, you should behave as if ***every*** **meeting recording (online or in-person) requires:**

1. **Clear, prior Notice** that you're recording *and* using an AI note-taker, and
2. **Explicit, all-party Consent**, with a real way to say no,

…plus include all the usual GDPR / transfer / vendor-management pieces in the background.

In many countries and U.S. States, failure to have all parties consent to a recording violates relevant laws.

This paper provides the detail, broken down to help you operationalize this as a DPO.

[1] https://www.seyfarth.com/news-insights/workplace-recordings-and-eavesdropping-limiting-criminal-and-legal-liabilities.html
[2] Covert recordings in the workplace - HCR Law
[3] https://employersfederation.org/audio-recording-of-meetings-are-you-complying-with-data-protection-obligations/
[4] https://www.privacypolicies.com/blog/meeting-recording-disclaimers/
[5] https://gdpr-info.eu/art-6-gdpr/
[6] https://gdpr-info.eu/art-7-gdpr/
[7] https://www.seyfarth.com/news-insights/workplace-recordings-and-eavesdropping-limiting-criminal-and-legal-liabilities.html

2 The Legal Landscape in One View

We're sitting at the intersection of three regimes:

1. **US Wiretap / Recording Laws**
    - Federal law (Wiretap Act) generally allows recording with **one-party consent** – at least one participant must know and agree.[8]
    - **About a dozen+ US states** require **all-party consent** to record "confidential" conversations or calls (often called "**two-party consent**"). Lists differ by source[9], but consistently include **CA, DE, FL, IL, MD, MA, MT, NH, PA, WA**, and often **CT, NV, MI, VT** with various nuances.[10][11]
2. **EU / UK Data-Protection + Telecom Rules**
    - **GDPR / UK GDPR** govern any processing of personal data in recordings and transcripts (audio, video, chat, notes).[12]
    - The **ePrivacy Directive and national telecom/wiretap laws** protect the **confidentiality of communications** – listening to or recording calls / online meetings is "interference" that is only lawful under narrow conditions (consent or specific legal basis).[13][14]
    - In some countries (e.g. **Germany**), **secretly recording a private conversation is a criminal offense** (§201 StGB).[15][16]
3. **Modern Privacy / Wiretap Litigation (US & EU)**
    - **California's CIPA** and similar laws are being used aggressively against companies that record calls or digital interactions without *prior* consent, including where third-party vendors "intercept" communications.[17][18]
    - EU Data Protection Authorities (e.g. **Danish DPA**) have held that **mere disclosure that "calls may be recorded for training" is not enough** – affirmative consent is required in many scenarios.[19][20]

Because meetings today often mix **US + EU participants + third-party AI tools**, the safest workable baseline is: **all-party, explicit consent + GDPR-grade transparency** for every recording.

---

[8] https://www.justia.com/50-state-surveys/recording-phone-calls-and-conversations/
[9] https://hostie.ai/resources/state-by-state-call-recording-compliance-ai-virtual-hosts-2025
[10] https://worldpopulationreview.com/state-rankings/two-party-consent-states
[11] https://knowledge.hubspot.com/calling/what-are-the-call-recording-laws
[12] https://gdpr-info.eu/art-6-gdpr/
[13] https://www.edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en
[14] https://usercentrics.com/knowledge-hub/eprivacy-everything-you-need-to-know-about-it/
[15] https://privacyrights.org/resources-tools/law-overviews/california-invasion-privacy-act-cipa
[16] https://heydata.eu/en/magazine/balancing-trust-and-control-how-to-make-ai-recorded-online-meetings-gdpr-compliant/
[17] https://privacyrights.org/resources-tools/law-overviews/california-invasion-privacy-act-cipa
[18] https://www.reuters.com/legal/legalindustry/cipa-lawsuits-escalate-businesses-marketers-scramble-mitigate-risk--pracin-2025-11-25/
[19] https://www.clarip.com/blog/danish-dpa-consent-customer-service-recording/
[20] https://www.ballardspahr.com/insights/alerts-and-articles/2019/04/denmark-dpa-rules-on-how-gdpr-applies-to-voice-recordings

3 United States – Notice & Consent Duties

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

3.1 Federal Wiretap Act

- **18 U.S.C. § 2511** requires Consent from at least one party to record a conversation; recording with criminal or tortious intent is prohibited.[2122]
- In practice, if someone from your company is participating and knows/approves the recording, *federal* law is satisfied – but that's **not enough** because of *state* laws.

3.2 State Recording Laws (online & in-person)

1. **One-Party States** (majority of states)
    - Only one participant needs to consent; the recorder's own consent is enough.
    - Recording can still be unlawful if it's "confidential" and you are a *non-party* intercepting without any party's consent (think vendor "listening in" without disclosure).[23]
2. **All-Party / Two-Party States**
    - Roughly **11–15 states** treat many calls or private conversations as requiring consent from **all** parties, including **at least**:
      CA, DE, FL, IL, MD, MA, MT, NH, PA, WA, and commonly **CT, NV, MI, VT** in some contexts.[242526]
    - Some have quirks:
        - **Connecticut**: all-party for *electronic* recordings, one-party for many in-person conversations.[27]
        - **Oregon**: one-party for electronic comms, two-party for in-person conversations in private places.[28]
3. **Multi-State Meetings**
    - Courts often apply the **stricter law** when a more protective state like California is involved (e.g. *Kearney v. Salomon Smith Barney* for CA vs GA calls).[29]
    - For **distributed online calls**, you should assume that **if any participant is in an all-party state, you must get all-party, prior consent.**
4. **Practical "Notice vs Consent"**

---

[21] https://www.justia.com/documents/50-state-surveys-recording-calls-and-conversations.pdf
[22] https://www.justia.com/50-state-surveys/recording-phone-calls-and-conversations/
[23] ibid.
[24] https://worldpopulationreview.com/state-rankings/two-party-consent-states
[25] https://knowledge.hubspot.com/calling/what-are-the-call-recording-laws
[26] https://hostie.ai/resources/state-by-state-call-recording-compliance-ai-virtual-hosts-2025
[27] https://en.wikipedia.org/wiki/Telephone_call_recording_laws
[28] https://www.avoma.com/blog/call-recording-laws
[29] https://www.mwl-law.com/wp-content/uploads/2018/02/RECORDING-CONVERSATIONS-CHART.pdf

- In many states, **clear notice + continued participation** can count as *implied* consent (e.g. "This call is being recorded; if you do not consent, please hang up").
- Given litigation trends and AI vendors sitting in the middle, it's safer to aim for **explicit consent** (verbal "yes", checkbox, or written acceptance) for **any recorded meeting with US participants**.

3.3 CIPA and Modern Wiretap-style Lawsuits

- **California Invasion of Privacy Act (CIPA)** requires **all-party consent** to record "confidential communications" (phone and electronic) and is the basis for many high-value class actions (statutory damages up to $5,000 per violation).[30][31]
- Plaintiffs are now attacking things like **pixels, session replay, chatbots and AI "listeners"** as ***unlawful interception*** when vendors receive communications without **prior, explicit consent**.[32][33]

Implication for AI Note-takers:

If your AI meeting tool (Granola, Otter, Fireflies, MeetGeek, Krisp, Lindy, Read AI, or others) receives audio in real time, plaintiffs could argue it is a ***third-party interceptor*** analogous to session replay tools. So:

- You want **clear, pre-meeting Disclosure** ("Notice") that a third-party AI service will receive content.
- You want **affirmative Consent** from participants **before** any recording starts, not just a buried line in a privacy policy.

[30] https://privacyrights.org/resources-tools/law-overviews/california-invasion-privacy-act-cipa
[31] https://pmc.ncbi.nlm.nih.gov/articles/PMC7234701/
[32] https://www.reuters.com/legal/legalindustry/cipa-lawsuits-escalate-businesses-marketers-scramble-mitigate-risk--pracin-2025-11-25/
[33] https://iapp.org/resources/article/us-litigation-series-website-tracking/

4 Europe (EEA + UK) – Notice, Consent and Lawful Basis

In Europe, the threshold is higher: you're not just asking "can I record", but **"on what legal basis can I process this data at all?"**

4.1 GDPR Lawful Basis for Meeting Recordings

Every recording/transcript needs a legal basis under **Art. 6 GDPR/UK GDPR**. Common candidates[34][35]:

1. **Consent (Art. 6(1)(a))**
    - Must be **freely given, specific, informed, unambiguous**, and withdrawable.[36][37]
    - **Employees** are a special case: Data Protection Authorities (DPA) and the EDPB regularly say ***consent*** in employment is **often <u>not</u> "freely given"** because of power imbalance. You can still use it in some truly optional contexts (e.g., voluntary training webinars), but you need a credible "no" path.
2. **Legitimate Interests (Art. 6(1)(f))**
    - Often used for **business-need recordings** (e.g. documenting key decisions, training, quality).
    - Requires a **three-part test** (interest, necessity, balancing), recently further clarified by the EDPB in new legitimate interest guidelines.[38][39]
    - In the **employment context**, oversight bodies expect a **documented LIA + DPIA** for systematic monitoring (like routine recording of internal meetings).[40][41]
3. **Legal Obligation / Regulatory Requirement (Art. 6(1)(c))**
    - Certain regulated sectors (e.g. investment services in the EU) are legally required to record some calls and online meetings; in those cases, recording can be **mandatory**, but you still need to **inform participants**.[42][43]
4. **Special Categories (Art. 9)**
    - Recordings can easily capture **health data, union membership, political opinions, religious beliefs, etc.**

[34] https://gdpr-info.eu/art-6-gdpr/
[35] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/
[36] https://gdpr-info.eu/issues/consent/
[37] https://iapp.org/news/a/how-do-the-rules-on-audio-recording-change-under-the-gdpr
[38] https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf
[39] https://gdprlocal.com/gdpr-employee-monitoring/
[40] ibid.
[41] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
[42] https://eb-sim.de/en/data-protection-information-for-online-meetings/
[43] https://www.iea.nl/sites/default/files/2021-09/Data%20Protection%20Information%20for%20Video%20Calls%2C%20Online%20Conferences%2C%20Meetings%2C%20and%20Recordings.pdf

- Where that's likely, you probably need **explicit Consent** under Art. 9(2)(a) *or* another narrow Art. 9 basis (e.g. legal claims).[4445]

4.2 ePrivacy + National Wiretap / Criminal Law

- The **ePrivacy Directive** and national laws protect **confidentiality of electronic communications** – listening to, tapping, or storing communications is only allowed in narrow, defined circumstances.[4647]
- Many Data Protection Authorities (DPA) treat **call/meeting recording for "training" or "quality"** as needing **prior, explicit consent**, not just legitimate interests:
  - The **Danish DPA** required **affirmative consent** for customer service call recording for training; simple disclosure was not enough.[4849]
- **Criminal Law Overlay**
  - In **Germany**, recording private conversations without all parties' consent is a **criminal offense** (§201 StGB).[5051]
  - Similar prohibitions exist in other EU countries; **covert workplace recording** has led to lawful dismissals and, in some cases, criminal exposure.[5253]

Result: for EU/UK participants, you typically need:

- **Clear, prior Notice** that the meeting will be recorded and fed to an AI system, and
- Either:
  - **Valid Consent** (especially for training/quality/HR meetings or if sensitive data is likely), or
  - A **well-documented Legitimate-Interest** or **Legal-Obligation case**, plus a genuine **right to object** and an alternative for those who do.

4.3 Employee Monitoring Angle

Routine recording of internal meetings is treated as a form of **employee monitoring**, which triggers:

- Expectation of **DPIA**[54] (systematic monitoring).[5556]

---

[44] https://gdpr-info.eu/issues/consent/
[45] https://www.dickinson-wright.com/news-alerts/the-gdpr-covers-employee-hr-data-and-tricky
[46] https://www.edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en
[47] https://usercentrics.com/knowledge-hub/eprivacy-everything-you-need-to-know-about-it/
[48] https://www.clarip.com/blog/danish-dpa-consent-customer-service-recording/
[49] https://www.ballardspahr.com/insights/alerts-and-articles/2019/04/denmark-dpa-rules-on-how-gdpr-applies-to-voice-recordings
[50] https://www.lewik.org/term/15703/violation-of-the-privacy-of-the-spoken-word-section-201-german-criminal-code/
[51] https://heydata.eu/en/magazine/balancing-trust-and-control-how-to-make-ai-recorded-online-meetings-gdpr-compliant/
[52] https://en.wikipedia.org/wiki/Telephone_call_recording_laws
[53] https://www.cloudtalk.io/blog/is-call-recording-legal/
[54] https://www.linkedin.com/pulse/pia-vs-dpia-understanding-differences-when-conduct-each-scott-foote-u4wie/
[55] https://gdprlocal.com/gdpr-employee-monitoring/
[56] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

- Strong requirements for **Transparency, Proportionality, Data Minimization and Limited Retention**.[57][58]
- In some countries (e.g., **Germany, France**), possible duties to **inform and consult *works councils* or *unions*** *before* deploying AI note-takers as standard tooling.

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

[57] ibid.
[58] https://www.monitask.com/en/blog/gdpr-requirements-for-employee-monitoring-a-comprehensive-guide

5 AI Meeting Assistants – Controller/Processor & Transfer Issues

5.1 Who is the Controller?

For most organizations (SMBs to multi-national enterprises):

- **Your company is almost always the Controller** of employees' and customers' personal data in the recording & transcript.
- The **AI note-taker provider** is usually a **Processor**, but many (including Granola, Otter, Fireflies, MeetGeek, Krisp, Lindy, Read AI, or others) also describe themselves as a controller for some processing (analytics, model training, security, etc.).[59][60]

Practical obligations:

- You need a **Data Processing Agreement (Art. 28 GDPR)** that:
  - Clearly ***restricts*** the vendor's use of data (especially for model training).
  - Defines sub-processors, security measures, retention, deletion, and audit rights.

5.2 International Transfers (EU → US)

Most well-known tools (including Granola, Otter, Fireflies, MeetGeek, Krisp, Lindy, Read AI, or others) store transcripts on **US-based cloud providers (AWS US)**.[61][62]

Vendor	Default Hosting (Publicly Documented)	EU Data Residency Option?
Granola.ai	US AWS	❌ No
Otter.ai	US AWS	⚠️ GDPR compliance via DPF/SCCs but no regional EU-only hosting
Fireflies.ai	US (Google/AWS)	✔ Yes — via enterprise "Private Storage"
MeetGeek.ai	Likely US	❓ Not publicly documented
Krisp.ai	Likely US	❌ No clear EU hosting
Lindy.ai	❓ Unknown	❓ Contact vendor
Read.ai	❓ Unknown	✔ Claimed EU/other regions per user reports

For EU/UK data subjects, transfer of personal information to the U.S. is a **Restricted Transfer**. Options:

1. **EU–US Data Privacy Framework (DPF)**

[59] https://help.granola.ai/article/privacy-policy
[60] https://www.granola.ai/security
[61] https://help.granola.ai/article/privacy-policy
[62] https://www.granola.ai/security

- Since **July 2023**, there's an EU adequacy decision for US companies ***certified* under DPF**, and the EU General Court upheld the framework in Sept 2025.[63][64][65]
- If your vendor is DPF-certified **under the relevant list (EU, UK, Swiss)**, transfers can be based on that.

2. **Standard Contractual Clauses (SCCs)**
   - If not DPF-certified, you need SCCs + a **transfer risk assessment** and any necessary **supplementary measures**, as per EDPB Recommendations 01/2020.[66][67]

Either way, the fact that **AI models may be trained (even on de-identified data)** must be reviewed for **re-identification risk** and clearly **disclosed**.

[63] https://www.dataprivacyframework.gov/Program-Overview
[64] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en
[65] https://www.reuters.com/sustainability/boards-policy-regulation/eu-court-backs-latest-data-transfer-deal-agreed-by-us-eu-2025-09-03/
[66] https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[67] https://www.edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en

6 What You *Must* Do Around Notice & Consent

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

6.1 Before Using any AI Note-Taker Org-wide

As DPO, I'd treat this as a **"high-risk new processing" project** and do:

1. **Data-Mapping & Scoping**
    - What meetings will be recorded? (internal stand-ups vs. HR 1:1s vs. customer calls)
    - What exactly is captured? (audio only; video; screens; chat; shared documents)
    - Who has access to raw recordings vs. summaries?
2. **DPIA + Legitimate Interest Assessment**
    - Especially for employee meetings and where recording becomes "the default".
    - Document why you need recordings rather than just human notes, and how you minimize impact.
3. **Vendor Assessment & Data Processing Agreements (DPA)**
    - Specifically address security (encryption, access controls, logging), model-training use, data residency, sub-processors.[68][69]
4. **Global Policy Decision**
    - Decide which **meeting types** are:
        - **Always recorded** (with stricter safeguards)
        - **Optional** (only with express consent of participants)
        - **Never recorded** (e.g. disciplinary, grievance, whistleblowing).
5. **Shadow IT Control**
    - Explicitly **ban personal AI note-takers** (personal Granola, Otter, Fireflies, MeetGeek, Krisp, Lindy, Read AI, etc.) for work calls **unless** approved and configured in line with policy.[70][71]

6.2 What Notice Must Contain (GDPR-grade Transparency)

For both **online and in-person meetings**, participants should be told, ***before*** recording starts:

1. **That recording is happening**, including:
    - Audio, video, screen share, chat, and whether the AI will also read shared docs.

---

[68] https://fellow.ai/blog/ai-meeting-assistant-security-and-privacy/
[69] https://meetgeek.ai/blog/ai-meeting-assistants-security-privacy
[70] https://fellow.ai/blog/ai-meeting-assistant-security-and-privacy/
[71] https://www.reddit.com/r/ArtificialInteligence/comments/1lxndp8/ethics_of_using_ai_notetaking_apps_at_work/

2. **That an AI service is being used**, including:
    - The provider's name (e.g. "Granola.ai"), and that they will receive the content.
3. **Purposes**
    - e.g. "capturing decisions and action items", "training staff", "legal/compliance logging", etc.
4. **Legal Basis**
    - Consent / legitimate interest / legal obligation, and, if legitimate interest, a short explanation.
5. **Retention Periods**
    - e.g. "full recordings kept 30 days; summaries retained 1 year."
6. **Access & Onward Disclosures**
    - Who in your org can access; whether data can be shared outside; whether the vendor uses de-identified data to train models.[72][73]
7. **Rights and Choices**
    - Right to **object** or **refuse consent**, alternatives if they do so, and how to request deletion.

This should be ensured via:

- A **dedicated Privacy Notice** for recordings / AI assistants (GDPR Art. 13), linked in invites.[74][75]
- **Short, in-meeting script** at the start of any recorded session.

6.3 Getting Valid Consent in Practice

To satisfy EU & strict US states simultaneously, design consent to be:

- **Prior** – before actual recording or AI capture begins.
- **Affirmative** – no reliance on silence.
- **Specific** – separate from general terms / generic privacy policy.
- **Recorded** – so you can prove it.

Concrete Options:

1. **Calendar invite + join page**
    - Add a line like:

[72] https://help.granola.ai/article/privacy-policy
[73] https://www.granola.ai/security
[74] https://www.iea.nl/sites/default/files/2021-09/Data%20Protection%20Information%20for%20Video%20Calls%2C%20Online%20Conferences%2C%20Meetings%2C%20and%20Recordings.pdf
[75] https://www.mdc-berlin.de/content/data-protection-notice-online-meetings-teleconferences-and-online-seminars-zoom

"*This meeting may be recorded and transcribed using [Tool]. By joining, you acknowledge the privacy notice [link]. We'll confirm at the start and you may decline being recorded.*"

That sets expectation, but is **not enough alone** for EU or all-party states.

2. **In-meeting verbal Consent (online or in-person)**

Example script that will play well globally:

"*Before we begin: this meeting will be recorded and transcribed using an AI note-taker, [Tool]. That means your audio and any shared content may be captured and stored by [Company] and processed by [Tool vendor] on our behalf.*

We'll use the recording only to [brief, specific purposes]. We keep full recordings for [X] days and summaries for [Y]. Access is restricted to [who].

If you don't want to be recorded, please say so now – we can pause the recording for specific parts or arrange an alternative.

Do you consent to the recording and AI processing?"

- For small meetings, you can **record each "yes"** in the audio.
- For larger calls/webinars, use a **poll / click-through** in the conferencing tool and treat **non-responders as *no*** for EU participants.

3. **In-person signage + verbal reminder**

- Post signs at entrances / meeting rooms:

"*Audio/video recording and AI meeting transcription may be in use. Please speak to the organizer if you do not wish to be recorded.*"

- For small internal meetings, still **explicitly ask** at the start and log objections.

4. **Handling objections / non-consent**

If someone doesn't consent:

- **Option A:** Stop recording for that meeting.
- **Option B:** Allow them to stay but **mute / disable camera** for certain portions and make sure the AI tool **isn't capturing them** – this can be hard with desktop-level tools like Granola.[76]
- **Option C:** Provide an **alternative channel** (follow-up written summary, separate call without recording, etc.).

For EU employees, also clearly explain that **refusing consent has no negative consequences** (where you rely on consent) and document that in your DPIA.

[76] https://www.granola.ai/security

7 Data Retention, Deletion, and Legal Hold Issues w/ AI Meeting Assistants

AI note-taking services turn everyday conversations into durable records: audio, transcripts, summaries, action items, and sometimes even searchable indexes or "memory" features. That's powerful… but it also means your meeting content now has a real **data lifecycle** that you need to control.

Two capabilities sit at the center of doing this safely:

- specifying **retention** and **deletion schedules**, and
- placing and releasing **legal holds**.

7.1 Data Retention and Deletion

Being able to **set retention and deletion schedules** is foundational because meeting notes almost always contain **personal data** and often contain **sensitive business information** (strategy, pricing, HR topics, customer issues). If notes linger indefinitely "because the tool keeps them," you accumulate unnecessary **privacy risk**, **security risk**, and **compliance exposure**. A defensible retention policy lets you **match storage duration to purpose**: for example, short retention for raw recordings, longer for approved summaries, and "never retained" for certain meeting types. It also supports **privacy principles** like **data minimization** and **storage limitation**, and it **reduces the blast radius** if there's ever an account compromise or vendor incident.

Just as important is **deletion that actually deletes**… not only the visible transcript, but also derivatives: summaries, highlights, speaker labels, sentiments, attachments, and any secondary data stores (indexes, caches, exports, backups where feasible, and third-party sub-processors). Without reliable deletion mechanisms and auditability, you as the Data Controller can't confidently honor internal policies, contractual commitments, or data subject requests… and you can't prove you did what you said you'd do.

7.2 Establishing and Releasing Legal Holds

On the flip side, you also need the ability to **establish legal holds** over meeting notes when litigation, investigations, or audits are reasonably anticipated. Legal holds are the "brakes" on deletion: they prevent routine retention policies from destroying potentially relevant records. If you can't preserve the right meetings quickly and precisely… by date range, project, custodian, or specific meeting ID… you risk **spoliation claims**[77], **sanctions**, or **credibility damage**, and you make **eDiscovery** far more **expensive** and **chaotic**.

Finally, legal holds must be **releasable**. Once the matter ends, you need to lift the hold and **allow normal retention to resume**… otherwise holds become a backdoor for indefinite retention. The best setups make this easy to manage with clear scope, logging, and defensible workflows that coordinate Legal, Privacy, and Security:

- **retention** as the **default** rule,
- **legal holds** as a **controlled exception**, and
- both **enforced consistently** across the AI note-taking stack.

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

[77] https://content.next.westlaw.com/practical-law/document/I0fa034abef0811e28578f7ccc38dcbee/Spoliation?viewType=FullText&transitionType=Default&contextData=(sc.Default)

8 Special Points for In-Person Meetings

The legal framework is basically the same – it's still processing of personal data and often "listening in" to communications – but a few practical nuances:

- **Hidden devices** (phones on the table, laptop apps listening to room audio) are high-risk: in many EU countries (and all-party US states), this is effectively **criminal or civil eavesdropping** without consent.[78][79]
- If you use **fixed room systems** (microphones, 360° cameras), you may fall under **video-surveillance / audio-monitoring guidance**; EDPB's video-device guidelines emphasize proportionality, signage, and limited retention.[80][81]
- In workplaces, permanent "always-on" recording of meeting rooms will almost never pass a DPIA unless you're in a heavily regulated / safety-critical context.

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

[78] https://www.lewik.org/term/15703/violation-of-the-privacy-of-the-spoken-word-section-201-german-criminal-code/
[79] https://pmc.ncbi.nlm.nih.gov/articles/PMC7234701/
[80] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
[81] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf

9 Putting This into a Workable Global Standard

If you want one policy that works across your US & European SMBs, a pragmatic template would be:

1. **Policy Baseline**
    - **No covert recordings – ever.**
    - **All-party, prior consent** required for any recording or AI transcription of meetings, regardless of jurisdiction.
    - **Higher bar for HR, performance, and disciplinary meetings** – default is **no recording**, with rare, tightly justified exceptions.
2. **Governance Controls**
    - Approved list of **recording / AI tools** (with DPAs and transfer mechanisms in place).
    - **Technical enforcement** where possible (e.g., admin settings disabling recording except for authorized users).
    - **Checks in onboarding** of new tools that touch audio/video.
3. **Documentation**
    - DPIA & LIA stored centrally.
    - Template **privacy notice for meetings**, updated per vendor.
    - Logging of **consent/objection events** (at least for higher-risk meetings).
4. **Training**
    - Short training for staff:
        - When they **may** record,
        - How to **say the script**, and
        - Why personal AI note-takers are **not allowed** without approval.

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.

10 Short, Practical Checklist

For each new meeting type or deployment, ask:

1. **Are any participants in the EU/UK or an all-party US state?**
    1. Yes. Treat as **all-party consent required**.
2. **Is this internal employee monitoring or HR-sensitive?**
    1. Yes. DPIA + likely **avoid recording** or require explicit consent.
3. **Will sensitive data probably come up?**
    1. Yes. Need an **Art. 9 basis** (usually explicit consent).
4. **Is the vendor US-based and processing EU data?**
    1. Yes. Check **DPF/SCCs**, sign Data Processing Agreements (DPA), do transfer impact assessment (TIA).
5. **Do we have a clear notice + documented consent mechanism?**
    1. No. Then, fix before launch.

CAVEAT: This author is not a lawyer, and you should consult your own general counsel or external privacy attorneys.